PROFESSIONAL SERVICES NETWORK • arem

Letna konferenca notranjih revizorjev javnega sektorja

Vloga notranjega revizorja pri obvladovanju strateških tveganj povezanih z informacijsko tehnologijo

2.6.2026

Urad RS za nadzor proračuna

Fakulteta za upravo

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP

renato@arem-psn.com

Za uvod – diskusija z udeleženci

- Katera so strateška tveganja IT tipične organizacije v javnem sektorju?

- Ali in kako se razlikuje javni sektor od gospodarstva glede obvladovanja strateških tveganj IT?

Kaj so strateška tveganja povezana z IT v javnem sektorju ?

- Svet
  - Evropa
    - Slovenija
      - Javni sektor

- Organizacija v javnem sektorju

Specifična tveganja – mikro vidik

Splošna tveganja – makro vidik

Splošna tveganja – makro vidik

Global risks ranked by severity, short term (2 years) and long term (10 years)

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

	Short term (2 years)	Long term (10 years)
1.	Geoeconomic confrontation	Extreme weather events
2.	Misinformation and disinformation	Biodiversity loss and ecosystem collapse
3.	Societal polarization	Critical change to Earth systems
4.	Extreme weather events	Misinformation and disinformation
5.	State-based armed conflict	Adverse outcomes of AI technologies
6.	Cyber insecurity	Natural resource shortages
7.	Inequality	Inequality
8.	Erosion of human rights and/or of civic freedoms	Cyber insecurity
9.	Pollution	Societal polarization
10.	Involuntary migration or displacement	Pollution

Source
World Economic Forum Global Risks Perception Survey 2025-2026

Risk categories
Economic · Environmental · Geopolitical · Societal · Technological

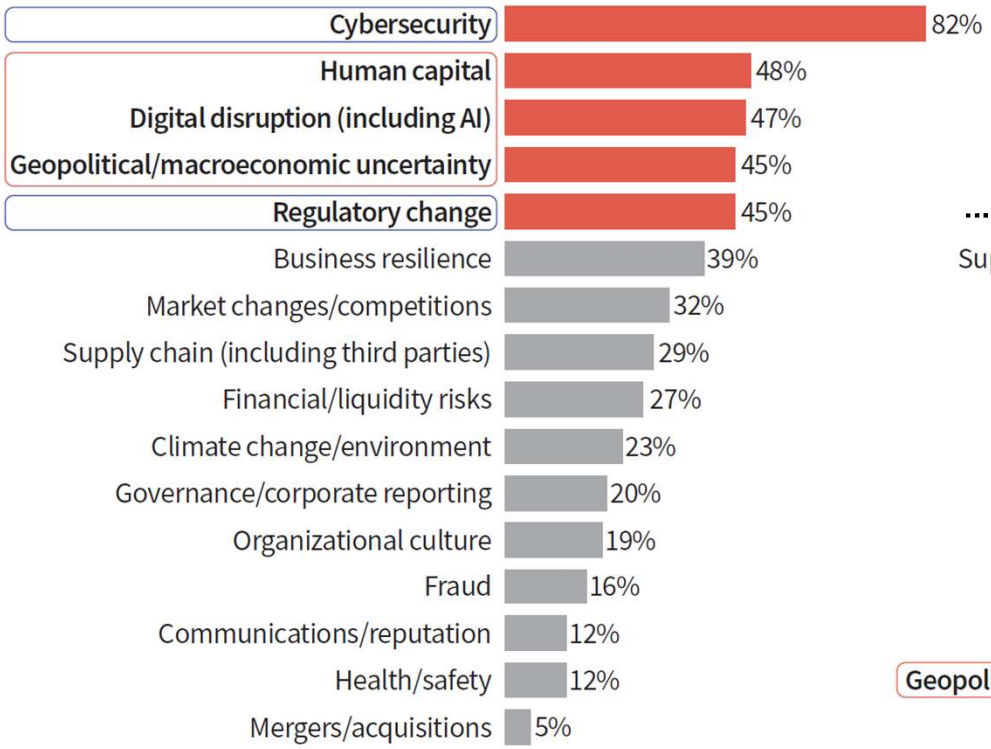
Splošna tveganja – makro vidik

EUROPE

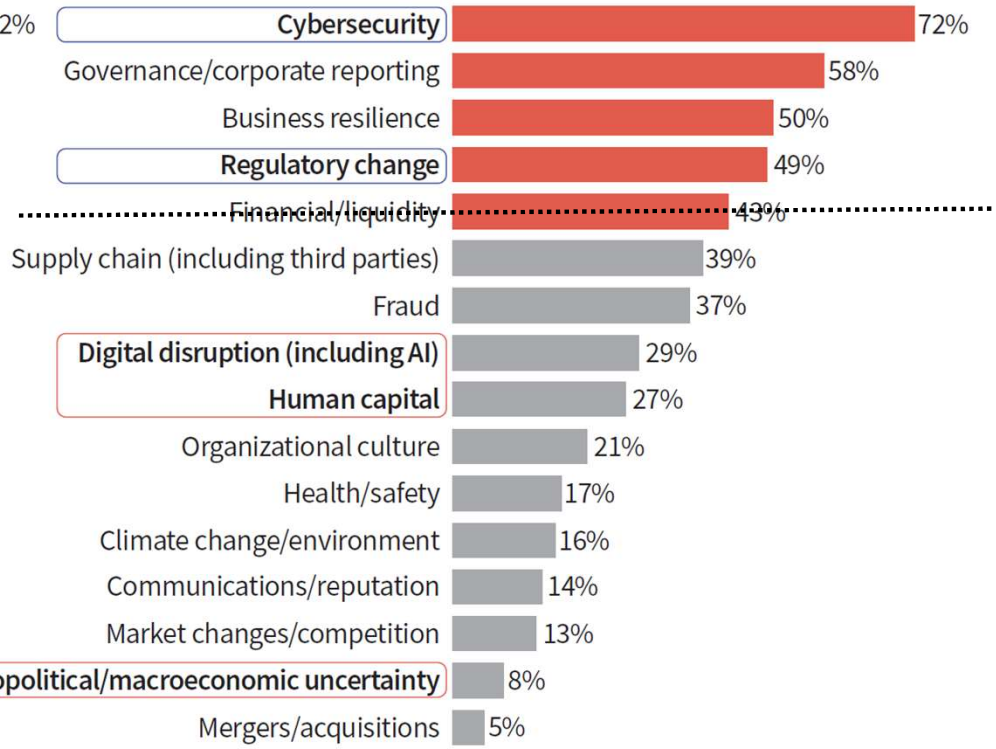
Exhibit 4.13. Europe – Risk vs. Audit Priorities

Survey questions: **What are the Top 5 risks your organization currently faces? (Choose 5.)**
What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)

Europe – Highest Risks



Europe – Highest Audit Priorities



Highest risks and audit priorities | Areas with both high risk and high audit priority | Areas with high risk but lower audit priority

Note: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 879 for Europe.

Splošna tveganja – makro vidik

EUROPE

Exhibit 4.12. Europe – Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	Change from 2024 to 2025	Change	Risk area
79%	74%	72%		-2	Cybersecurity
61%	64%	58%		-6	Governance/corporate reporting
50%	47%	50%		+3	Business resilience
50%	51%	49%		-2	Regulatory change
45%	40%	43%		+3	Financial/liquidity
36%	36%	39%		+3	Supply chain (including third parties)
36%	36%	37%		+1	Fraud
21%	23%	29%		+6	Digital disruption (including AI)
26%	28%	27%		-1	Human capital
21%	24%	21%		-3	Organizational culture
19%	18%	17%		-1	Health/safety
19%	20%	16%		-4	Climate change/environment
11%	14%	14%		0	Communications/reputation
10%	13%	13%		0	Market changes/competition
8%	6%	8%		+2	Geopolitical/macroeconomic uncertainty
9%	7%	5%		-2	Mergers/acquisitions

Increased audit priority compared to prior year Decreased audit priority compared to prior year

Note 1: Risk in Focus survey conducted online from April 28 to June 6, 2025, by the Internal Audit Foundation and partners. *n* = 879 for Europe.
Note 2: The orange and blue bars show the difference in audit priority ratings from 2024 to 2025. The column labeled "change" shows the percentage point difference between 2024 and 2025. The areas are listed from the highest to lowest audit priority rating for 2025. The years indicate the year the survey was conducted.

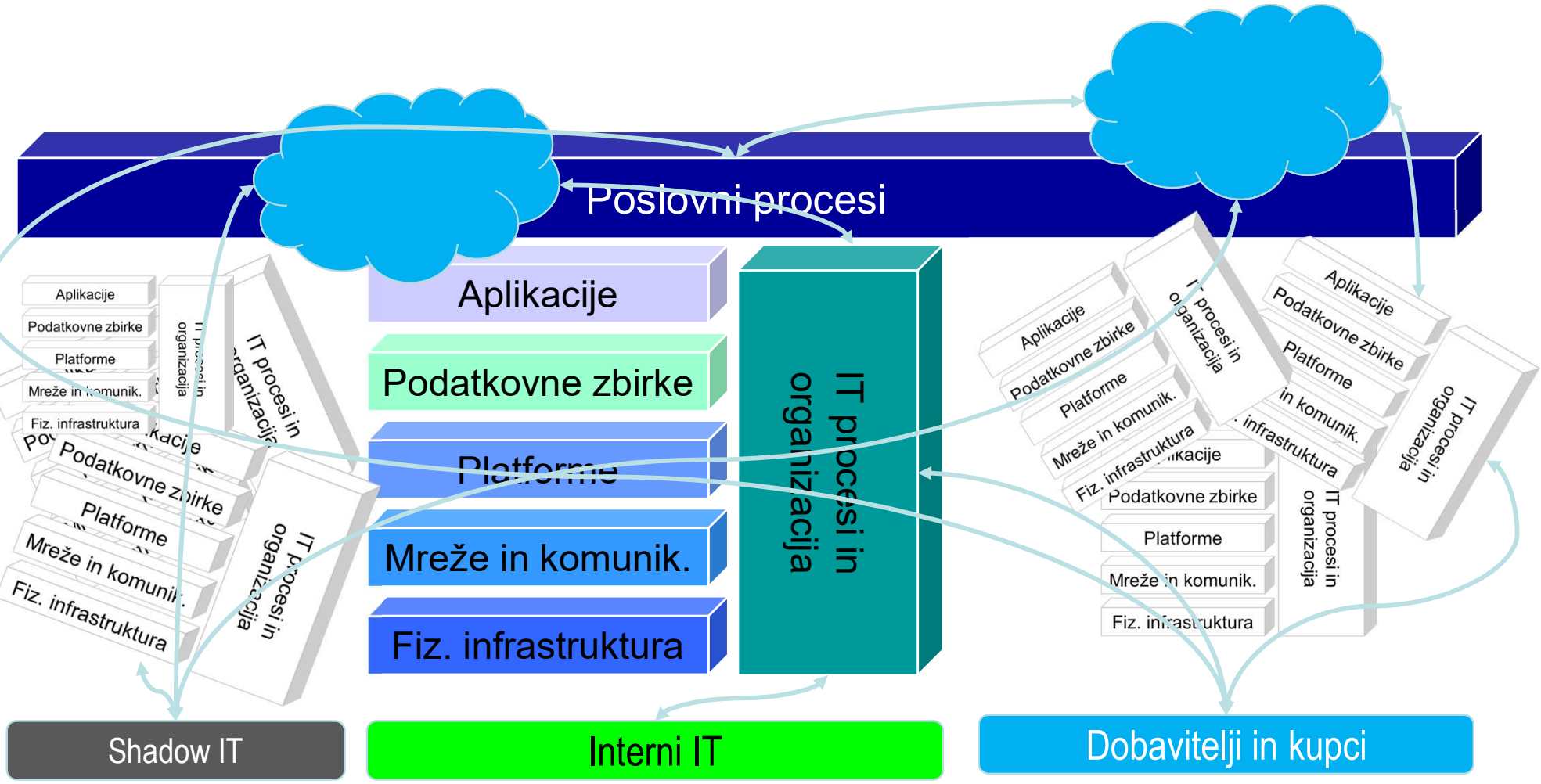
Primeri strateških IT tveganj

„Notranji revizor ni nujno tehnični specialist, mora pa razumeti poslovne posledice IT tveganj.“

- neuspešni digitalni projekti
- kibernetski napadi,
- izguba podatkov,
- odvisnost od ključnih dobaviteljev,
- neustrezno upravljanje umetne inteligence,
- zastarela infrastruktura,
- pomanjkanje kadrov,
- nedelujoči načrti neprekinjenega poslovanja,

Pripravil: Renato Burazer CISA, CISSP, CISM, CGEIT, CRISC

Kam dati fokus ?



Pripravil: Renato Burazer CISA, CISSP, CISM, CGEIT, CRISC

Nujen je premik iz operativnega pogleda na strateški

Ne samo ….

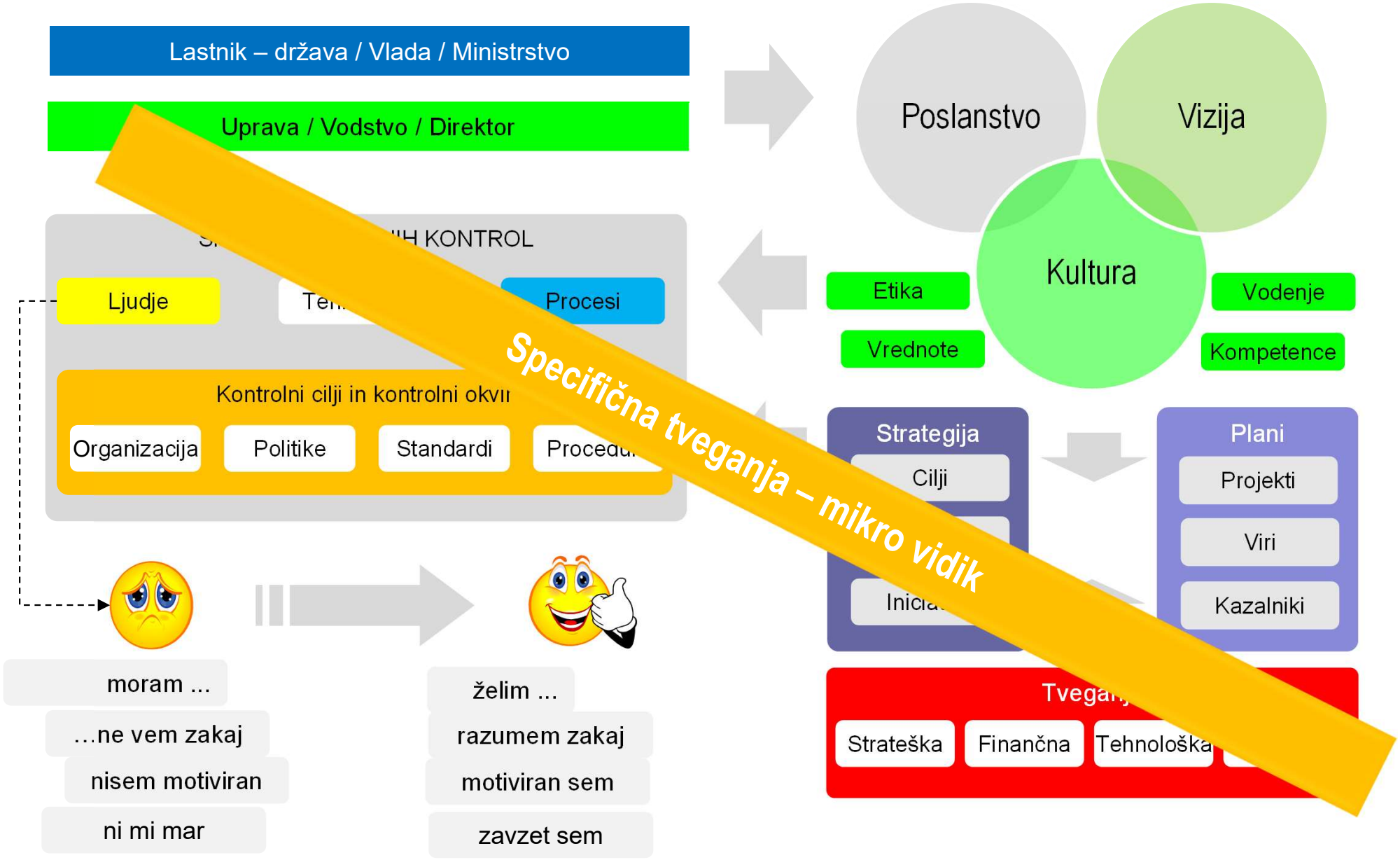
- ali obstajajo kontrole,
- ali so gesla dovolj dolga,
- ali so strežniki posodobljeni.

Ampak tudi …

- ali vodstvo razume ključna IT tveganja,
- ali so digitalni projekti povezani s strategijo,
- ali organizacija meri digitalna tveganja,
- ali obstajajo scenariji odpovedi kritičnih storitev,
- ali so vzpostavljeni ustrezni mehanizmi upravljanja IT

Pripravil: Renato Burazer CISA, CISSP, CISM, CGEIT, CRISC

Arhitektura – ene organizacije
Javni sektor



Specifična tveganja organizacije

Strateško tveganje | Okoljsko tveganje | Tržno tveganje | Kreditno tveganje | Operativno tveganje | Tveganje skladnosti

Tveganja povezana z informacijami in tehnologijo

S	O	S	O	S	O	S	O
Tveganje nezagotavljanja koristi/vrednosti IT		Tveganje izvedbe IT programov in projektov		Tveganje IT operacij in izvajanja storitev		Kibernetsko in informacijsko-varnostno tveganje	
• Ali so investicije v IT skladne s strategijo in nameni organizacije? • Ali investicije v IT ustvarjajo pričakovane koristi in vrednosti?		• Ali je izvedba IT programov in projektov zagotovljena v okviru predvidenih okvirov (čas, denar, kakovost, obseg, skladnost, drugo...) ?		• Ali je delovanje IT sistemov skladno s pričakovanji organizacije? • Ali je izvajanje storitev podprto z IT sistemi in storitvami primerno, učinkovito in uspešno v okviru merljivih tolerančnih vrednostih?		Ali je varnost informacijskih sredstev in vseh povezanih funkcij in procesov ustrezno obvladovana? Ali je zagotovljena ustrezna operativna (digitalna) odpornost na grožnje in motnje?	

Vir: RISK IT 2.0 ISACA, prevod in prilagoditev Renato Burazer

Notranja revizija

Storitve podajanja zagotovil

Svetovalne storitve

Upravljanje (Governance) IT:

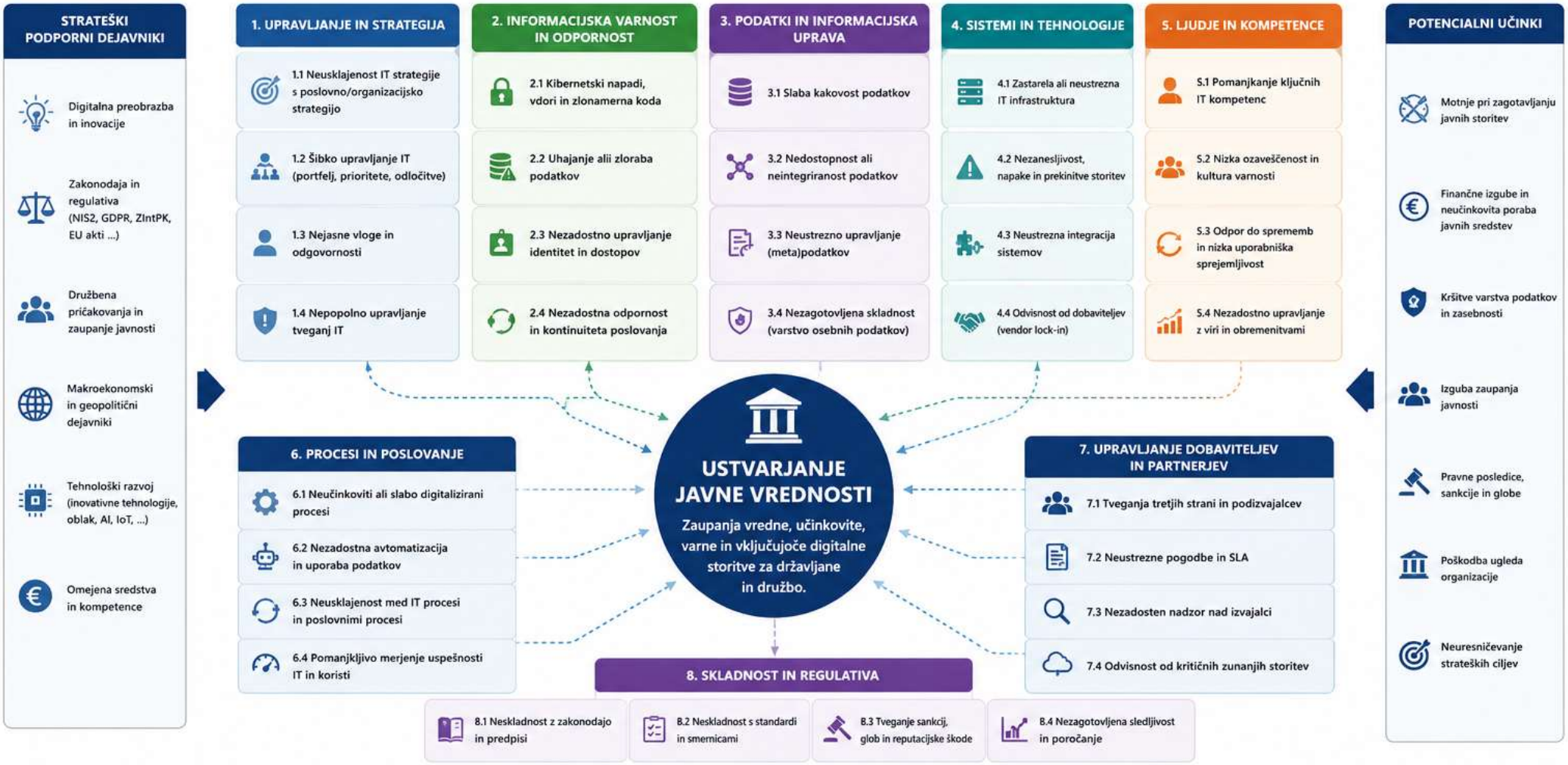
- **Strategije IT so usklajene s cilji organizacije.**
- **Vzpostavljen je proces upravljanja tveganj**, ki omogoča pravočasno prepoznavanje, obvladovanje in spremljanje IT-groženj.
- **Naložbe in viri v IT so optimizirani**, da organizaciji zagotavljajo največjo možno vrednost.
- **Vzpostavljeni so kazalniki (metrike)** za spremljanje in poročanje o uspešnosti delovanja IT.

Vodenje (Management) IT:

- **Uspešnost IT opredeljena, merjena in o njej poročano** z uporabo smiselnih in relevantnih kazalnikov.
- **Tveganja so ustrezno prepoznana in obvladovana**, vključno s komunikacijo z upravo oziroma nadzornim odborom.
- **IT viri so upravljani učinkovito in gospodarno.**

ZEMLJEVID STRATEŠKIH IT TVEGANJ – JAVNI SEKTOR

"Strateška IT tveganja izvirajo iz uporabe informacijskih tehnologij pri doseganju strateških ciljev organizacije in ustvarjanju javne vrednosti."



KATEGORIJE TVEGANJ PO NARAVI

Strateška | Operativna | Finančna | Skladnost | Informacijska varnost | Reputacijska

VIR TVEGANJ

Notranji dejavniki (procesi, ljudje, sistemi) | Zunanji dejavniki (tehnologija, grožnje, regulativa, dobavitelji) | Dogodki (namerni, nenamerni, nepredvideni)

KLJUČ DO USPEŠNEGA UPRAVLJANJA TVEGANJ

Prepoznaj → Ovrednoti → Obvladaj → Spremljaj → Poročaj → Izboljšuj

Opomba: Zemljevid je prilagojen za uporabo v javnem sektorju in temelji na dobrih praksah (IIA IPPF, COBIT 2019, ISO/IEC 27001, NIST, ITIL, ISO 31000).

Vir: RB, Ustvarjeno z orodjem UI ChatGPT

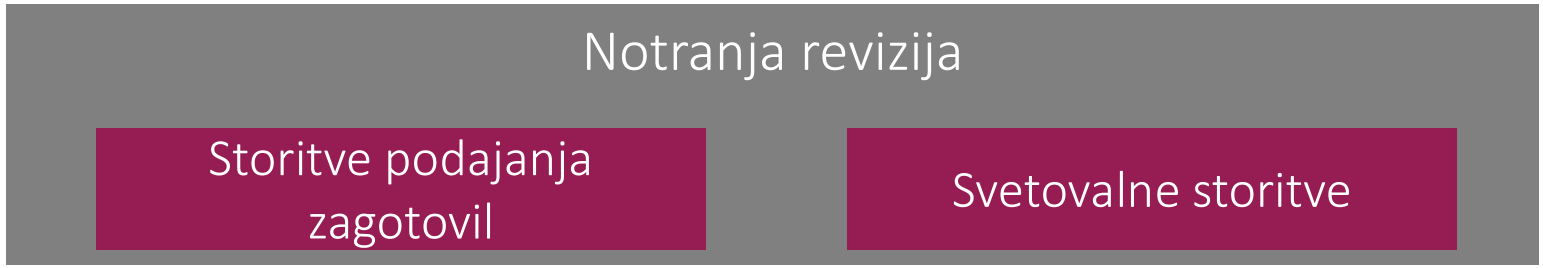
Pripravil: Renato Burazer CISA, CISSP, CISM, CGEIT, CRISC

Zaključne misli

- Notranji revizor ni nujno tehnični specialist, mora pa razumeti poslovne posledice IT tveganj.

- Notranja revizija mora pomagati odgovoriti organizaciji na vprašanje:
  - Ali organizacija razume IT tveganja in obvladuje na ravni, ki omogoča doseganje strateških ciljev?

- Notranji revizor prihodnosti ne presoja zgolj kontrol. Presoja sposobnost organizacije, da varno, odgovorno in trajnostno deluje v digitalnem okolju.



Vprašanja in diskusija danes ali kdaj drugič, vabljeni.

Renato Burazer
managing partner, CISA, CISSP, CISM, CGEIT

Tel.: +386 41 33 56 77
renato@arem-psn.com

PROFESSIONAL SERVICES NETWORK • arem

www.arem-psn.com/si

www.arem-psn.com